IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA,		
v.	|	CRIMINAL CASE NUMBER:
PAMELA MOZEE	|	1:15-CR-00434-WSD-JSA

FINAL REPORT AND RECOMMENDATION AND ORDER

Defendant in this drug trafficking case moves to suppress [24] the proceeds of a search warrant issued relating to her internet email account. This warrant was issued by a Magistrate Judge in Alaska for records held by an internet service provider in California. Defendant's only argument is that the warrant exceeded the geographic scope of the issuing judge's powers under the applicable statutes and procedural rules, because it called for a search outside of the boundaries of the District of Alaska. This argument is meritless and Defendant's Motion [24] should be **DENIED**.

DISCUSSION

On October 28, 2014, United States Magistrate Judge Deborah M. Smith, sitting in the District of Alaska, issued a search warrant authorizing the search of an email account associated with the Defendant maintained by Yahoo! Inc., based in Sunnyvale, California. [24-1] at 1. Defendant argues that this warrant was "invalid *ab initio*" for having been issued outside the geographic limitations of

Magistrate Judge Smith's authority.

The authority of United States Magistrate Judges emanates generally from the Federal Magistrates Act of 1968, 28 U.S.C. §636.[1] Section 636(a) states that:

> Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law– (1) all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure[.]

28 U.S.C. §636(a).

Rule 41(b)(1), Fed.R.Crim.P. governs a Magistrate Judge's search warrant authority generally. This Rule provides certain geographic limitations as follows:

> A magistrate judge with authority in the district – or if none is reasonably available, a judge of a state court of record in the district – has authority to issue a warrant to search for and seize a person or property located within the district.

Rule 41 provides limited specific circumstances in which a Magistrate Judge may authorize searches outside of the district, but it is undisputed that none of those circumstances apply here.[2]

---

[1] Congress subsequently changed the title from "Magistrate" to "Magistrate Judge" in the Judicial Improvements Act of 1990.

[2] *See* Fed.R.Crim.P. 41(b)(2) (authorizing searches for property within the district at the time of the issuance of the warrant even if the property is outside the district by the time of the search); (b)(3) (authorizing searches outside the district in terrorism investigations); (b)(4) (authorizing use of tracking devices installed within the district, even if the premises being tracked leaves the district during the tracking period); (b)(5) (authorizing searches in U.S. territories, possessions,

It is true, therefore, that Rule 41 did not authorize Magistrate Judge Smith, sitting in the District of Alaska, to issue a warrant authorizing a search to take place in the Northern District of California. Rule 41, however, expressly states that "[t]his rule does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances." Fed.R.Civ.P. 41(a)(1).

As the Government correctly points out, Congress provided independent statutory for the search authorized by Magistrate Judge Smith. The Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, includes various provisions specifically addressed to the methods by which law enforcement agencies may seek to obtain, and the authority the courts have to approve, records of stored wire and electronic communications. Specifically, 18 U.S.C. § 2703 provides that a government entity may require a provider of electronic communications or remote computing services to disclose the contents of stored wire or electronic communications, and other information, by way of a warrant using the procedures described in the Federal Rules of Criminal Procedure, issued "by a court of competent jurisdiction." 18 U.S.C. § 2703(a)&(b).

The term "court of competent jurisdiction" is a statutorily-defined term, which includes "any district court of the United States (including a magistrate

---

commonwealths, diplomatic or consular facilities or residences).

judge of such court)," that *either* "has jurisdiction over the offense being investigated," *or* is in the judicial district where the service provider is located or where the records are stored. *See* 18 U.S.C. § 2711(3)(A)(i)-(ii). In other words, the SCA specifically provides that a U.S. Magistrate Judge may issue a search warrant for the contents of electronic communications to an electronic communications provider or provide of remote computing services, where the provider and records are located outside the Judge's district, so long as the court in that district has "jurisdiction over the offense being investigated."

The Defendant's argument that "A magistrate judge's authority to issue a search warrant is clearly limited to items located within the judge's federal district," [24] at 3, is therefore wrong on the facts of this case. While this may be a correct statement as to the limits of a judge's authority under Rule 41, this argument fails to address the broader geographic authority conferred by the SCA in the context of a search warrant for stored electronic communications from an appropriate service provider. *See United States v. Bansal*, 663 F.3d 634, 662 (3d Cir. 2011) (rejecting argument that "Rule 41(b), which limits a Magistrate Judge's jurisdiction to the District in which he or she sits, trumps § 2703(a)."); *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) (The geographic limitation of

Rule 41(b) does not apply to warrants under the SCA).[3]

Defendant does not argue that Yahoo! Inc. fails to qualify as a provider of electronic communications or remote computing services. Indeed, the agent's affidavit states that Yahoo! Inc. provides electronic mail communications services. *See* Gov't Ex. A ¶ 20. Nor does Defendant argue that the District of Alaska lacked jurisdiction over this offense. Indeed, the agent's affidavit establishes apparent illegal distributions of controlled substances via mail delivery *in Alaska*. *See id.* ¶¶ 10-18.[4] *See In re Search Warrant*, 2005 WL 3844032, *4-5 (M.D. Fla. Feb. 13, 2006) (reference to "jurisdiction over the offense being investigated" refers to

---

[3] To be sure, the SCA requires that any warrant be issued "using the procedures described in the Federal Rules of Criminal Procedure." 18 U.S.C. § 2703(a). Defendant does not argue that this language somehow incorporates Rule 41's geographic limitations. In any event, this is clearly not the case. To infer Rule 41's geographic limitations into § 2703 by way of this language would contradict the clear statutory provisions. Congress clearly stated that any courts in districts with "jurisdiction over the offense" may issue warrants under the SCA, and Congress obviously understood that these districts may not always be where the service provider and/or data is located. This is clear, because Congress defined "court of competent jurisdiction" as *either* a district with jurisdiction over the investigation, *or* the district where the provider or data is located. This disjunctive phrasing would be meaningless if only the district where the data and/or provider were located could issue a warrant. Of course this makes sense, because there is no logical reason why all warrants for stored communications from Yahoo!, Microsoft, Google, Facebook, Twitter, and other silicon valley and San Francisco-based providers, relating to all investigations worldwide, should all have to be processed through the Northern District of California.

[4] Obviously, criminal conduct may cross the boundaries of districts such that more than one district might have jurisdiction over an offense or series of offenses.

"crimes that occur in [the issuing court's] district.")

Defendant's authority, *United States v. Levin*, 2016 WL 2596010 (D. Mass. May 5, 2016), is inapt. In that case, a court suppressed the use of a computer technique, authorized by a U.S. Magistrate Judge in Virginia, that essentially allowed a government computer in Virginia to hack into and report back information about a suspected child pornographer's computer based in Massachusetts. *Id.* at *2-*4. *Levin* did not involve a warrant to a provider of remote computing or electronic communications services, such as Yahoo! Inc. Therefore, the Government did not invoke the authority of the SCA, and the court in *Levin* analyzed the Magistrate Judge's authority solely under Rule 41. This analysis has no bearing here.

Thus, Magistrate Judge Smith enjoyed authority under the SCA to issue this warrant. Notably, Defendant does not address the SCA or respond at all to Defendant's specific citations. The Motion to Suppress therefore should be **DENIED.**

CONCLUSION

It is **RECOMMENDED** that Defendant's Motion to Suppress [24] be **DENIED**. Defendant's Motions to Suppress Statements [23] [25] are **DEFERRED** to the District Judge. The case is otherwise **READY FOR TRIAL**.

IT IS SO RECOMMENDED AND ORDERED this 14th day of June, 2016.

JUSTIN S. ANAND
UNITED STATES MAGISTRATE JUDGE